

## UNITED STATES DISTRICT COURT

for the  
Central District of California

In the Matter of the Search of )

(Briefly describe the property to be searched or identify the )  
person by name and address) )

Case No. 23-MJ-6472

The common areas and the bedroom used by )  
Sophia Shaklian at 5432 Barton Avenue, Apt. )  
8, Los Angeles, CA 90038 )  
)  
)

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California (*identify the person or describe the property to be searched and give its location*):

*See Attachment A*

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (*identify the person or describe the property to be seized*):

*See Attachment B*

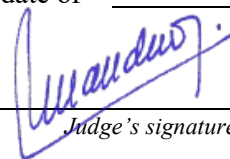
Such affidavit(s) or testimony are incorporated herein by reference.

**YOU ARE COMMANDED** to execute this warrant on or before 14 days from the date of its issuance (*not to exceed 14 days*)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.


Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (*check the appropriate box*)

☐ for \_\_\_\_ days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.Date and time issued: December 18, 2023 at 7:27 pm  
Judge's signatureCity and state: Los Angeles, CAHon. Maria A. Audero, U.S. Magistrate Judge  
Printed name and titleAUSA: Jason C. Pang, x2652

AO 93C (Rev. 8/18) Warrant by Telephone of Other Reliable Electronic Means (Page 2)

<b>Return</b>		
Case No.: Case No. 23-MJ-6472	Date and time warrant executed: 12/18/2023 at approximately 7:30 PM	Copy of warrant and inventory left with: Sophia Shaklian
Inventory made in the presence of : FBI Special Agent John Gasper		
Inventory of the property taken and name of any person(s) seized: <ul style="list-style-type: none"> <li>One box of documents related to Mabel Imaging, Inc.</li> </ul>		
<b>Certification</b>		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: 12/19/2023	<div style="text-align: center;">             Executing officer's signature         </div> <div style="text-align: center; margin-top: 10px;">           Lucas Alfaro, Special Agent            Printed name and title         </div>	

**ATTACHMENT A**

PREMISES TO BE SEARCHED

The SUBJECT PREMISES consists of the common areas and bedroom used by Sophia Armenuhi Shaklian located at 5432 Barton Avenue, Apartment 8, Los Angeles, California 90038. The SUBJECT PREMISES is the residence of Sophia Shaklian and includes offices, safes, containers, and other parts therein, as well as any patio, porch, balcony, or any garage or storage room associated with or assigned to SUBJECT PREMISES. The SUBJECT PREMISES is located in a two-story, multi-unit apartment complex located on the east side of Barton Avenue. The building has numbers "5432" on the front of the building that faces north on Barton Avenue. The SUBJECT PREMISES is further described as Apartment 8, which is on the second floor, and southeast corner of the building.

The photograph below is of 5432 Barton Avenue, Los Angeles, CA 90038.



**ATTACHMENT B**

**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1347 (Health Care Fraud), 18 U.S.C. § 1028A (Aggravated Identity Theft), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire and Health Care Fraud), 18 U.S.C. § 1956 (Money Laundering and Conspiracy to Launder Money), and 18 U.S.C. § 1957 (Transactional Money Laundering) (collectively, "the Subject Offenses"), namely:

a. For the time period beginning March 1, 2019, and continuing to the present:

i. Clinical files and patient records for all Medicare patients on whose behalf claims were submitted to Medicare by any of the following Medicare providers: MABEL IMAGING INCORPORATED ("MABEL").

ii. Records or communications pertaining to the preparation of medical records for MABEL, such as internal correspondence, lists, or notes containing patient personal information (such as names, addresses, contact information, dates of birth, social security numbers, Medicare numbers, and Medicare eligibility); lists or notes regarding missing or incomplete medical records for MABEL, including nursing notes, referral orders, test orders or results, or certifications of terminal illness; and evidence of the mailing or other sharing

of such documents with other persons or receipt of such documents from other persons for MABEL.

iii. Partially completed forms or drafts, pre-printed forms or templates for preparing clinical records, and pre-signed blank forms pertaining to MABEL.

iv. Records or communications pertaining to Medicare billing, including correspondence with Medicare or any Medicare contractor related to Medicare patients or Medicare billing; correspondence and communications with billing services, consultants, advisors, and other persons about the proper preparation and submission of claims or supporting documentation to Medicare; billing manuals, bulletins, newsletters, articles, notices, memoranda, lists of procedure codes, price sheets, copies of rules or regulations, and instructions or directions relating to billing Medicare; supporting documentation for any claims to be submitted; and Medicare remittance notices or explanations of benefits.

v. Records or communications pertaining to any inspection, review, audit, or inquiry into MABEL by Qlarant, any other Medicare contractor, or Los Angeles County Department of Health Services ("LADHS"), and memoranda notes, correspondence, and e-mails concerning any such inspection, review, audit, or inquiry.

vi. Records or communications pertaining to the owners and operators of MABEL, including individuals who perform managerial or billing roles regardless of title, and including

records identifying the individuals filling those roles or providing contact information for them.

vii. Records or communications pertaining to personnel and payroll or service files and records for employees and independent contractors of, or other individuals paid by MABEL, including identification cards or passports; employee lists; and documents reflecting names, addresses, duration of employment or service, pay schedules, W-2s, 1099s, invoices, duties, and reasons for separation or termination from employment.

viii. Records or communications pertaining to work schedules, time sheets, appointment books, patient visit logs or route sheets, invoices, and other records showing the services provided by and all payments made to or for doctors, registered nurses, licensed vocational nurses, physical therapists, social workers, aides, marketers, community liaisons, x-ray and imaging technicians, and other persons or companies purportedly providing services to Medicare patients on behalf of MABEL.

ix. Records or communications pertaining to Medicare patient eligibility verification logs checking eligibility of MABEL or on behalf of MABEL.

x. Records or communications pertaining to presentations, marketing, or advertisements on behalf of MABEL; marketers and other patient referral sources for MABEL; the referral source of any of MABEL; any contracts, agreements, or documents referencing written or verbal contracts with marketers

or other patient referral sources for MABEL; and any payments made, in cash or in kind, or other consideration given to marketers or other patient referral sources on behalf of MABEL or in relation to MABEL.

xi. Records or communications pertaining to contracts and any professional service agreements purportedly provided to or by any consulting or professional service companies in relation to MABEL.

xii. Records or communications pertaining to any notary or notary services sought or obtained in relation to MABEL.

xiii. Records or communications pertaining to the finances of MABEL, including accounting records; profit and loss statements; tax records including tax returns and records relating to consultation with tax preparation services; bank applications, login, password, and account information; bank statements, checks, ATM and/or debit cards, signature stamps, tokens, and deposit items; records of financial transactions, including wire transactions and money transmittal receipts; cash receipts and disbursement journals and ledgers; expense accounts; loan documents and notes; and records pertaining to the disposition of any assets, including individuals receiving funds from MABEL, purchase and investment records, financing applications and records, and escrow records.

2. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.



3. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device; and

g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

5. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

**II. SEARCH PROCEDURES FOR HANDLING POTENTIALLY PRIVILEGED INFORMATION**

6. The following procedures will be followed at the time of the search in order to avoid unnecessary disclosures of any privileged attorney-client communications or work product:

Non-Digital Evidence

7. Prior to reading any document or other piece of evidence ("document") in its entirety, law enforcement personnel conducting the investigation and search and other individuals assisting law enforcement personnel in the search (the "Search Team") will conduct a limited review of the document in order to determine whether or not the document appears to contain or refer to communications between an attorney, including Patric Hooper, David S. Schumacher, or other individuals associated with the law firm Hooper, Lundy & Bookman, P.C., or to contain the work product of an attorney and any person ("potentially privileged information"). If a Search Team member determines that a document appears to contain potentially privileged information, the Search Team member will not continue to review the document and will immediately notify a member of the "Privilege Review Team" (previously designated individual(s) not participating in the investigation of the case). The Search Team will not further review any document that appears to

contain potentially privileged information until after the Privilege Review Team has completed its review.

8. In consultation with a Privilege Review Team Attorney ("PRT Attorney"), if appropriate, the Privilege Review Team member will then review any document identified as appearing to contain potentially privileged information to confirm that it contains potentially privileged information. If it does not, it may be returned to the Search Team member. If a member of the Privilege Review Team confirms that a document contains potentially privileged information, then the member will review only as much of the document as is necessary to determine whether or not the document is within the scope of the warrant. Those documents which contain potentially privileged information but are not within the scope of the warrant will be set aside and will not be subject to further review or seizure absent subsequent authorization. Those documents which contain potentially privileged information and are within the scope of the warrant will be seized and sealed together in an enclosure, the outer portion of which will be marked as containing potentially privileged information. The Privilege Review Team member will also make sure that the locations where the documents containing potentially privileged information were seized have been documented.

9. The seized documents containing potentially privileged information will be delivered to the United States Attorney's Office for further review by a PRT Attorney. If that review reveals that a document does not contain potentially privileged information, or that an exception to the privilege applies, the document may be returned to the Search Team. If appropriate based on review of particular documents, the PRT Attorney may apply to the court for a finding with respect to the particular documents that no privilege, or an exception to the privilege, applies.

#### Digital Evidence

10. The Search Team will search for digital devices capable of being used to facilitate the subject offenses or capable of containing data falling within the scope of the items to be seized. The Privilege Review Team will then review the identified digital devices as set forth herein. The Search Team will review only digital device data which has been released by the Privilege Review Team.

11. The Privilege Review Team will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location.

12. The Privilege Review Team and the Search Team shall complete both stages of the search discussed herein as soon as

is practicable but not to exceed 180 days from the date of execution of the warrant. The government will not search the digital device(s) beyond this 180-day period without obtaining an extension of time order from the Court.

13. The Search Team will provide the Privilege Review Team with a list of "privilege key words" to search for in the content records, to include specific words like "Patric Hooper," "David S. Schumacher," "Hooper, Lundy & Bookman, P.C.," or their email addresses, and generic words such as "privileged" and "work product." The Privilege Review Team will conduct an initial review of all of the content records by using the privilege key words, and by using search protocols specifically chosen to identify content records containing potentially privileged information. The Privilege Review Team may subject to this initial review all of the data contained in each digital device capable of containing any of the items to be seized. Documents or data that are identified by this initial review as not potentially privileged may be given to the Search Team.

14. Documents or data that the initial review identifies as potentially privileged will be reviewed by a Privilege Review Team member to confirm that they contain potentially privileged information. Documents or data that are determined by this review not to be potentially privileged may be given to the Search Team. Documents or data that are determined by this

review to be potentially privileged will be given to the United States Attorney's Office for further review by a PRT Attorney. Documents or data identified by the PRT Attorney after review as not potentially privileged may be given to the Search Team. If, after review, the PRT Attorney determines it to be appropriate, the PRT Attorney may apply to the court for a finding with respect to particular documents or data that no privilege, or an exception to the privilege, applies. Documents or data that are the subject of such a finding may be given to the Search Team. Documents or data identified by the PRT Attorney after review as privileged will be maintained under seal by the investigating agency without further review absent subsequent authorization.

15. The Search Team will search only the documents and data that the Privilege Review Team provides to the Search Team at any step listed above in order to locate documents and data that are within the scope of the search warrant. The Search Team does not have to wait until the entire privilege review is concluded to begin its review for documents and data within the scope of the search warrant. The Privilege Review Team may also conduct the search for documents and data within the scope of the search warrant if that is more efficient.

16. In performing the reviews, both the Privilege Review Team and the Search Team may:

- a. search for and attempt to recover deleted, "hidden," or encrypted data;
- b. use tools to exclude normal operating system files and standard third-party software that do not need to be searched; and
- c. use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

17. Neither the Privilege Review Team nor the Search Team will seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

18. The Search Team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

a. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

b. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.



c. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

d. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

e. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

19. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the

custody and control of attorneys for the government and their support staff for their independent review.

20. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.